Office of the Inspector General
U.S. Department of Justice

Audit of the Federal Bureau of Investigation's Implementation of Its Next Generation Cyber Initiative

Audit Division 15-29 July 2015

AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S IMPLEMENTATION OF ITS NEXT GENERATION CYBER INITIATIVE

EXECUTIVE SUMMARY

The Federal Bureau of Investigation (FBI) has reported that the frequency and impact of cyber attacks on private sector and government computers increased dramatically in the last decade and are expected to continue to grow. In January 2012, former FBI Director Mueller stated during a congressional testimony that he expected the cyber threat to surpass the terrorism threat to our national security in the years to come. According to current FBI Director, James B. Comey, Jr., the FBI is prioritizing the investigation and prevention of cyber intrusions against the United States. The FBI has designated the protection of the United States against cyber-based attacks and high-technology crimes as its number three priority, behind only counterterrorism and counterintelligence.

Following the Office of the Inspector General's (OIG) April 2011 report on the FBI's ability to address the national cyber intrusion threat, in October 2012 the FBI launched its Next Generation Cyber (Next Gen Cyber) Initiative to enhance its ability to address cybersecurity threats to the United States.[1] In fiscal year 2014, the FBI initially budgeted $314 million for its Next Gen Cyber Initiative, including a total of 1,333 full-time positions (including 756 agents). In addition, the Department of Justice (Department) requested an $86.6 million increase in funding for fiscal year 2014 to support the Initiative. The objective of this audit was to evaluate the FBI's implementation of its Next Gen Cyber Initiative.

In our 2011 report, the OIG made 10 recommendations to improve the FBI's efforts in this area, including that the FBI establish policies and procedures for the sharing of information at the National Cyber Investigative Joint Task Force (NCIJTF); enhance efforts to educate FBI field office personnel on the NCIJTF's role and use within FBI's national security cyber strategy; evaluate the effectiveness of the step-by-step training course for FBI agents on how to investigate national security intrusion cases; reconsider the rotation policy for cyber agents and ensure that agents skilled and experienced in cyber intrusions are available to FBI field offices; and consider developing regional hubs with agents that are experts in investigating national security intrusions.

The Next Gen Cyber Initiative is an ongoing, multi-year strategy that included two fundamental changes to the way the FBI addresses cyber threats. First, the FBI narrowed the focus of its Cyber Division to work solely on cyber intrusions because the FBI determined that they pose the greatest threat to national security. Simultaneously, the FBI transferred non-intrusion programs

[1] U.S. Department of Justice Office of the Inspector General, *The Federal Bureau of Investigation's Ability to Address the National Security Cyber Intrusion Threat,* Audit Report 11-22 (April 2011).

previously run by the Cyber Division, including the Innocent Images National Initiative addressing child pornography and the Intellectual Property Rights Program, to its Criminal Investigative Division (CID). Second, the FBI shifted its cyber intrusion emphasis from reacting to cyber-attacks to predicting and preventing them. In the context of this new framework, the Next Gen Cyber Initiative focuses on four areas: (1) strengthening the NCIJTF; (2) advancing the capability of the FBI cyber workforce and supporting related enterprise infrastructure; (3) expanding the Cyber Task Forces focused on intrusion investigations in each of the FBI's 56 field offices, and (4) enhancing information sharing and operational collaboration with the private sector.

Our current audit found that the FBI has made considerable progress towards achieving the goals it established for the Next Gen Cyber Initiative. We found that the NCIJTF, which serves as a coordination, integration, and information sharing center among 19 U.S. agencies and international representatives for cyber threat information, is no longer perceived as an extension of the FBI. Additionally, according to NCIJTF partners, information sharing has improved among the members, which was an issue identified in our 2011 report. Also, the FBI has established Cyber Task Forces in all 56 field offices. In 2011, the FBI had Cyber Crime Task Forces in 45 of the 56 field offices. Furthermore, the FBI has implemented a cyber-specific training strategy to improve the technical skills of its entire workforce, with specific training made available to those working cyber intrusion investigations. The FBI is offering qualified personnel an opportunity to participate in a Master's Degree program at Carnegie Mellon University and is in the process of initiating a similar program at New York University's Polytechnic School of Engineering, to provide an attractive incentive and valuable training to help recruit, develop, and retain the cadre of FBI cyber professionals.

While the FBI has made progress in implementing its initiative, we found that there are still issues preventing the FBI from fully meeting all of its goals for the Next Gen Cyber Initiative. In particular, we found that:

- the NCIJTF did not have a process to measure the timeliness of information sharing among members;

- recruitment and retention of qualified candidates remain a challenge for the FBI, as private sector entities are often able to offer higher salaries and typically have a less extensive background investigation process;

- the FBI has encountered challenges in attracting external participants to its established Cyber Task Forces;

- the FBI did not hire 52 of the 134 computer scientists for which it was authorized; and

- 5 of the 56 field offices did not have a computer scientist assigned to that office's Cyber Task Force.

Finally, although the FBI is working to develop strategies to enhance outreach to private sector entities, it continues to face challenges partnering and sharing information with these entities. While the FBI has developed reports to provide the private sector with actionable information to allow it to protect its networks and to disseminate technical information gleaned from some ongoing investigations, both FBI and private sector representatives acknowledged to us that information sharing remains a challenge. We found that when the private sector shares information with the FBI, it is perceived by the private sector as akin to sending information into a black hole because they often do not know what becomes of it. We also found that the private sector is reluctant to share information with the government based on concerns regarding balancing national security and individual privacy interests. The private sector reluctance to share information has been further affected by the distrust of government created by the Edward Snowden leaks.[2] Private sector representatives have also expressed privacy concerns about how the information collected will be used. Additionally, information the FBI shares with the private sector is often considered by the recipients to be not useful because it is already known, lacks context, or is outdated.

While the FBI continues to advance its cyber capabilities, we found that it still needs to: (1) continue to focus its efforts on recruiting and retaining highly-skilled, technically trained cyber professionals; (2) increase external partners' participation on the Cyber Task Forces, including enhancing state and local law enforcement and interagency participation; and (3) expand private sector outreach to develop an environment that promotes information sharing and collaboration. We believe that the FBI needs to address these challenges to most effectively identify and address emerging cyber intrusion threats.

This report contains eight recommendations to assist the FBI in meeting these objectives and achieving the goals of the Next Gen Cyber Initiative that are the basis for its efforts to address this significant and growing threat to our national security.

[2] Edward Snowden is an American computer professional who worked at the National Security Agency as a contractor and revealed classified information, including details of United States government global surveillance programs. Snowden has been charged by the Department of Justice with violating the Espionage Act and theft of government property. United States v. Edward J. Snowden, 1:13 CR 265 (CMH).

AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S IMPLEMENTATION OF ITS NEXT GENERATION CYBER INITIATIVE

TABLE OF CONTENTS

AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S IMPLEMENTATION OF ITS NEXT GENERATION CYBER INITIATIVE

INTRODUCTION

The Federal Bureau of Investigation (FBI) has reported that both the frequency and the impact of cyber-attacks on our nation's private sector and government networks have increased dramatically over the past decade. In September 2014, FBI Director James B. Comey, Jr. testified that the FBI is prioritizing the investigation and prevention of intrusions against the United States, including botnets, state-sponsored hackers, and global cyber syndicates, and that the FBI is working to predict and prevent attacks rather than simply react after an attack has occurred.[3] As a result, the FBI has designated the protection of the United States against cyber-based attacks and high-technology crimes as its number three priority, behind only counterterrorism and counterintelligence.

The FBI has found that the range of actors conducting intrusions is as complex as it is varied. These cyber actors include spies from nation-states who seek secrets and intellectual property; organized criminals who want to steal personal identities and money; terrorists intent on attacking the power grid, water supply, or other infrastructure; and "hacktivists" who are politically motivated to make a statement through their conduct. The FBI investigates all of these types of attacks to determine the actors responsible for the intrusions.

For example, in October 2014, the FBI released an alert indicating that it had high confidence that highly skilled Chinese government-affiliated cyber actors were routinely stealing high value information from United States companies and government agencies. Also, according to a December 2014 FBI press release, the FBI initiated an investigation of a cyber attack on Sony Pictures Entertainment. The FBI investigation concluded that the North Korean government was responsible for the cyber attack. While stating that it has seen a wide variety and increasing volume of cyber intrusions, the FBI indicated that the destructive nature of the Sony Pictures Entertainment attack set it apart because it reflected the intent of a hostile foreign government to inflict significant harm on a United States business and suppress the right of United States citizens to free speech within our own

[3] James B. Comey, Jr., Director, Federal Bureau of Investigations, before the Homeland Security Committee, U.S. House of Representatives, concerning 'Worldwide Threats to the Homeland' (September 17, 2014).

Botnets are remotely controlled systems used to coordinate attacks and distribute phishing schemes, spam, and malware attacks. The FBI defines state-sponsored hackers as groups or individuals conducting computer network operations at the direction of, or with the support of, a nation state. Global cyber syndicates are organized criminal groups who use spam, spyware and malware, and other types of cyber tools to engage in criminal conduct, including identity theft, online fraud, and computer extortion for monetary gain.

borders and beyond. The FBI's most recent major initiative to strengthen its cyber capabilities to address attacks such as these is the Next Generation Cyber Initiative.

Background

In April 2011, the Department of Justice Office of the Inspector General (OIG) issued a report that addressed the FBI's ability to address the national security cyber intrusion threat.[4] The report made 10 recommendations to the FBI to help it to improve its efforts in this area, including that the FBI establish policies and procedures for the sharing of information at the National Cyber Investigative Joint Task Force (NCIJTF); enhance efforts to educate FBI field office personnel on the NCIJTF's role and use within FBI's national security cyber strategy; evaluate the effectiveness of the step-by-step training course for FBI agents on how to investigate national security intrusion cases; reconsider the rotation policy for cyber agents and ensure that agents skilled and experienced in cyber intrusions are available to FBI field offices; and consider developing regional hubs with agents that are experts in investigating national security intrusions. The FBI has provided the OIG with documentation to show that the FBI has adequately addressed all 10 of the recommendations contained in the 2011 report.

The FBI initiated its Next Generation Cyber (Next Gen Cyber) Initiative in May 2012 in order to enhance the FBI's ability to address the full range of cybersecurity threats to the United States. According to the FBI, implementation of the Next Gen Cyber Initiative has focused on four areas: (1) strengthening the NCIJTF; (2) advancing the capability of the FBI's cyber workforce and supporting related enterprise infrastructure; (3) expanding Cyber Task Forces in each of the FBI's 56 field offices that focus on intrusion investigations; and (4) enhancing information sharing and operational collaboration with the private sector.

The Next Gen Cyber Initiative represents a fundamental shift in the FBI's approach to addressing the cyber threat, changing its focus from reacting to cyber-attacks to predicting and preventing them. As part of the Next Gen Cyber Initiative, the Cyber Division was restructured to focus solely on computer intrusions and the FBI transferred responsibility for the investigation of crimes not focused on intrusion, specifically the Cyber Crime Program, Innocent Images National Initiative (addressing child pornography), Intellectual Property Rights, Internet Fraud, Internet Extortion, Identify Theft, Internet Money Laundering, and Internet Gambling, from the Cyber Division to the Criminal Investigative Division. The FBI-wide initiative encourages collaboration between the Cyber, Training, and Operational Technology Divisions and is supported by the Finance Division, Resource Planning Office, and Directorate of Intelligence. For fiscal year (FY) 2014, the FBI initially budgeted $314 million for its Next Gen Cyber Initiative, including a total of 1,333 full-time positions (including 756 agents). In addition, the Department of Justice (Department) requested an $86.6 million increase in funding

[4] U.S. Department of Justice Office of the Inspector General, *The Federal Bureau of Investigation's Ability to Address the National Security Cyber Intrusion Threat,* Audit Report 11-22 (April 2011).

for FY 2014 to support the Initiative. In this audit, we evaluated the FBI's implementation of its Next Gen Cyber Initiative in each of its four core areas.

Office of the Inspector General Audit Approach

The OIG conducted this audit to evaluate the FBI's implementation of the Next Gen Cyber Initiative to combat cyber intrusions. To accomplish this objective, we interviewed more than 50 FBI officials at FBI headquarters and FBI field offices. We also interviewed 3 Department of Justice officials, 10 NCIJTF members, and more than 12 private sector entities, including officials from the Carnegie Mellon University Software Engineering Institute and the National Cyber-Forensics and Training Alliance (NCFTA). We reviewed Next Gen Cyber Initiative planning documentation, records, and reports, and conducted five site visits to FBI field offices. The scope of our audit includes the implementation of the FBI's Next Gen Cyber Initiative from May 2012, when the initiative was announced, through January 2015.

In this report, the first finding describes the steps the FBI has taken to strengthen the NCIJTF, including changes to its organizational structure intended to ensure that the NCIJTF is no longer perceived as an extension of the FBI's Cyber Division and its efforts to foster interagency cooperation and information sharing. We interviewed 10 NCIJTF members, including representatives from the National Security Agency (NSA); the U.S. Department of Homeland Security (DHS); the Central Intelligence Agency (CIA); the Air Force Office of Special Investigations (AF-OSI); U.S. Cyber Command; and Five Eyes partners from Australia and the United Kingdom.[5]

In the second finding, we discuss the FBI's efforts to expand workforce training and enterprise infrastructure. Specifically, we reviewed the FBI's efforts to hire, train, and retain key cyber staff and the status of the FBI's efforts to fill cyber positions through January 2015. Additionally, we reviewed the FBI's new cyber training strategy to improve the skills of FBI employees, especially those working cyber intrusion investigations. Finally, we reviewed the challenges the FBI is facing in its effort to recruit and retain highly skilled cyber personnel, as well as the initiatives the FBI has planned to assist with addressing the challenges.

The third finding focuses on the expansion of the FBI's Cyber Task Forces in all of its 56 field offices and the FBI's efforts to recruit non-FBI participants to serve as Task Force Officers. To inform our review of the FBI's efforts in this regard, we conducted interviews with individuals from the following FBI field offices: Newark, New Jersey; Philadelphia, Pennsylvania; Pittsburgh, Pennsylvania; San Francisco, California; and Seattle, Washington. We also interviewed task force officers, including personnel from other law enforcement entities.

[5] Five Eyes (FVEY) is an alliance comprising Australia, Canada, New Zealand, the United Kingdom, and the United States.

The last finding describes information sharing and collaboration between the FBI and the private sector. We interviewed FBI officials, reviewed several FBI officials' testimonies related to the FBI's efforts to combat cyber intrusions, and interviewed individuals from private sector entities to gain an understanding of the FBI's efforts to enhance its information sharing and collaboration with the private sector. We also interviewed individuals from the FBI Cyber Division Operations and Outreach Section, including officials from the National Industry Partnership Unit (NIPU), Guardian Victim Analysis Unit (GVAU), and Key Partnership Engagement Unit (KPEU).

Appendix 1 contains further descriptions of our audit objectives, scope, and methodology.

FINDINGS AND RECOMMENDATIONS

National Cyber Investigative Joint Task Force

The FBI has made progress in strengthening the National Cyber Investigative Task Force (NCIJTF). NCIJTF members told us that information sharing between NCIJTF members has improved over the last several years. The NCIJTF is no longer perceived as an extension of the FBI's Cyber Division and instead it is seen as a multi-agency effort focused on coordinating, integrating, and sharing information related to domestic cyber threat investigations. But, the FBI should develop a process to track and measure the timeliness of information sharing.

National Cyber Investigative Joint Task Force

The National Cyber Investigative Joint Task Force (NCIJTF) was established by Presidential directive in 2008 to serve as the national focal point for the United States government to coordinate, integrate, and share information related to domestic cyber threat investigations.[6] Under the directive, the FBI was given the responsibility for developing and operating the NCIJTF. The NCIJTF currently co-locates members from 19 federal partners in the intelligence, law enforcement, and military sectors who collaborate and share intelligence about national security cyber threats and cyber actors.[7]

Strengthening the NCIJTF

One objective of the Next Gen Cyber Initiative was to strengthen the NCIJTF. To accomplish this objective, the FBI sought to formalize international participation and ensure the NCIJTF was no longer perceived by stakeholders as an extension of the FBI Cyber Division. In furtherance of this objective, we found that the NCIJTF was able to co-locate Five Eyes (FVEY) partners from Australia and the United Kingdom on a full-time basis and a representative from Canada on a part-time basis. As of January 2015, the NCIJTF was also working with New Zealand to bring a representative to the NCIJTF. We found the FBI has taken steps to remove the perception among its stakeholders, including interagency members, that the NCIJTF and FBI Cyber Division are synonymous. When the NCIJTF was formally established in 2008, the FBI's Cyber Division National Security Section and the

[6] National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (2008).

[7] In addition to 19 federal partners, the NCIJTF has five affiliates. Affiliates are agencies that have a signed memorandum of understanding with the NCIJTF and have personnel on site at the NCIJTF. However, the agencies do not have a primary cyber investigative role and their personnel do not have a primary role in NCIJTF campaigns.

NCIJTF functioned as a synonymous entity.[8] At that time, as we noted in our 2011 report, the NCIJTF was the headquarters component of the FBI's national security cyber efforts and the FBI appointed the Chief of the Cyber Division National Security Section to also serve as Director of the NCIJTF.[9] In addition, the NCIJTF functionally acted as the operational arm of the FBI's Cyber National Security Section.

Under the Next Gen Cyber Initiative the NCIJTF redirected its mission back to coordination, integration, and information sharing to better serve the law enforcement, intelligence, and military communities as a whole. Reflecting this change, the FBI revised the organizational structure of the NCIJTF, beginning in October 2012 with the formal separation of the FBI's Cyber Division operations from the NCIJTF and the designation of a dedicated NCIJTF Director. To further facilitate the separation, the NCIJTF incorporated representatives of non-FBI agencies into senior leadership positions at the NCIJTF. For example, a high ranking representative from the NSA was designated Principal Deputy Director of the NCIJTF in March 2014. We found that, as a result of these changes, the NCIJTF is no longer perceived by stakeholders as an extension of the FBI's Cyber Division. Further, NSA's elevation and commitment are notable given the finding in our 2011 report that the NSA was not a fully integrated partner in the NCIJTF.

In addition to redirecting its mission back to coordination and information sharing, the NCIJTF is also expanding its capabilities and increasing its staffing level. To accomplish this, the NCIJTF will be expanding its physical space. Currently, the NCIJTF is physically located in the same building as the Cyber Division's operational units. We were told by NCIJTF's Principal Deputy Director that the Cyber Division's operational units moved to a nearby location in January 2015. The FBI Cyber Division move is expected to free up valuable space and provide the NCIJTF with the opportunity to expand and strengthen its capabilities.

We believe that the organizational changes, including the designation of a high ranking dedicated NCIJTF Director, non-FBI agency participation in senior leadership, and the move of the FBI's Cyber Division operations to another location, should continue to further allow for the NCIJTF to establish itself outside of being seen as an extension of the FBI.

Information Sharing

In our 2011 report, we found that the FBI and other NCIJTF members did not consistently share cyber intrusion threat information with each other and that, where investigative information was not shared, NCIJTF members were not told

[8] The Cyber National Security Section, which due to reorganization no longer exists, was responsible for managing the FBI's counterterrorism and counterintelligence computer intrusion operations. The responsibility of the Cyber National Security Section has been divided amongst three newly-created sections in the Cyber Operations Branch.

[9] OIG, *National Security Cyber Intrusion Threat,* (April 2011).

why they did not receive available information. We also found a lack of coordination between FBI field offices and the NCIJTF regarding national security cyber intrusions, and that NCIJTF partners were not integrated into NCIJTF operations, with several of the partners not having a memoranda of understanding (MOU) in place establishing information sharing protocols among the NCIJTF members. The OIG made several recommendations related to these issues and the recommendations were closed after we verified that the FBI established NCIJTF information sharing policies and procedures for sharing information among all its members.

During this audit, NCIJTF members told us that they believe interagency collaboration has increased and information has been shared freely between member agencies as necessary. For example, the Operation Clean Slate Initiative was a continuous, targeted campaign aimed at eliminating significant botnets affecting United States interests. This initiative included United States government partners, international partners, and other private sector stakeholders. The NCIJTF members who we interviewed confirmed that there was significant and appropriate sharing of information between NCIJTF members in carrying out this initiative.

However, we were also told that the NCIJTF did not have a process to track and review the timeliness of such information sharing. We believe this is significant because if information sharing is delayed, the FBI cannot be certain NCIJTF members are able to use the information to effectively prevent or mitigate threats in a timely manner. Given the potentially negative impact outdated information can have on the NCIJTF's ability to effectively minimize or prevent a cyber attack, we believe that the FBI should develop a process to measure the timeliness of information sharing at the NCIJTF.

Cyber Workforce Development

An important objective of the Next Gen Cyber Initiative is to advance the capability of the FBI's cyber workforce. The FBI implemented a new training strategy to improve the technical skills of the entire FBI workforce, with specific training made available to those working cyber intrusion investigations. However, the FBI continues to encounter challenges recruiting, hiring, and retaining technically trained cyber personnel. The FBI also encountered challenges in hiring computer scientists to fill advanced technical skills positions in its field offices. FBI officials told us that it is difficult to compete with private sector entities that can offer higher compensation to individuals with highly technical cyber skills. The FBI background investigation process, which includes interviews, drug tests, and polygraph examinations, also excludes many candidates that otherwise meet the educational qualifications. FBI officials also told us that the 2013 federal budget sequestration and a government-wide hiring freeze contributed to this challenge.

Recruitment and Retention

We found that the recruitment and retention of cyber personnel is an ongoing challenge for the FBI. One FBI Human Resources official told us that there is a huge disparity between the number of people recruited and the number of special agents or professional staff actually hired by the FBI, and he described hiring as a "funneling process." While the process may start with a recruitment event attended by 5,000 interested candidates, the inability of candidates to meet the FBI's specific eligibility criteria reduces that number to approximately 2,000 eligible candidates. Subsequently he told us that only about 2 candidates out of such a group are actually hired by the FBI. Another FBI official told us that the FBI loses a significant number of people who may be interested because of the FBI's extensive background check process and other requirements, such as all employees must be United States citizens and must not have used marijuana in the past 3 years, and cannot have used any other illegal drug in the past 10 years. Another factor may be that private sector entities are able to offer technically trained, cyber professionals higher salaries than the FBI can offer.

During our audit, the FBI provided us with information on recommended steps for addressing the current and anticipated workforce challenges. To address the key challenges, an FBI working group recommended several measures, which were being prioritized at the time of our audit work. Some of the steps proposed included supporting and encouraging mobility of personnel between the public and private sectors to bring knowledgeable and seasoned professionals back to the FBI. Another proposed measure was to refocus the Student Loan Repayment Program (SLRP) so that a greater percentage of it is used to assist financially in recruiting personnel into targeted positions. Other proposed steps included establishing high

school recruiting programs and targeted utilization of the FBI's University Education Program.[10]

The FBI's Human Resource Division is working with FBI divisions and field offices to develop recruiting programs to identify schools, universities, clubs, and professional organizations that focus on the development and promotion of cyber education and talent. One FBI official explained that the FBI is offering several incentives to recruit individuals including school loan repayment, reimbursement for continuing education, and hiring at higher salary levels on the general pay scale. He also added that the FBI is providing training opportunities for existing personnel including certifications and enrollment in the Carnegie Mellon University Master's program in Information Technology as retention tools. In addition, in December 2014, the FBI announced to its employees a similar program at the New York University Polytechnic School of Engineering. We were told that such advanced educational opportunities provide an attractive inducement for individuals with cyber skills to stay with the FBI and, as discussed below, they can provide a valuable training opportunity for them as well. Still, although recruitment and retention of skilled cyber professionals is challenging for the FBI, most of the FBI cyber agents we interviewed told us that it is the FBI's mission that motivates them to stay at the FBI rather than leave for more lucrative positions.

Training

One objective of the Next Gen Cyber Initiative was to improve the cyber skills of its employees. To achieve this objective, the FBI implemented a new training strategy in 2012. The cyber training strategy included: (1) High Technology Environment Training, an initiative to improve the technical skills and baseline technological knowledge of the entire FBI workforce; (2) commercially available training courses for cyber personnel so that they can maintain their skills; and (3) opportunities for qualified FBI personnel to earn a Master of Science degree in Information Technology. In addition, we reviewed the results of a 2013 FBI training survey conducted to gain a better understanding of the training needs of the cyber workforce.

High Technology Environment Training

To address the increasing role of computer technology in criminal activity and to enable its most technically skilled cyber agents to focus on the most complex cases, the FBI developed an enterprise-wide training curriculum called High Technology Environment Training (HiTET). According to the FBI, HiTET was designed to ensure that the FBI's Special Agents, Intelligence Analysts, and professional staff possess the basic technical capabilities to address the growing cyber threat in the broad array of investigations that include a cyber element, but may not be focused cyber investigations. The HiTET Overview course was designed

[10] The FBI established the University Education Program (UEP) to enable qualified employees in the Counterterrorism, Counterintelligence, Cyber, and Security Programs to earn advanced degrees. The UEP is a tuition reimbursement program.

to provide non-technical personnel with a working knowledge of the growing cyber threat and teach them basic cyber investigative techniques that do not require a high level of technical expertise. HiTET is provided through the FBI's web-based Virtual Academy, which includes other cyber training course opportunities ranging from introductory to intermediate and are commensurate with personnel assignment and roles. Another HiTET class titled "Obtaining and Analyzing Digital Records" teaches personnel techniques for retrieval of digital evidence. According to the FBI, when non-technical personnel have this capability, they can retrieve data on their own in appropriate circumstances, thus allowing the FBI's most technically skilled cyber agents and specialists to concentrate on issues that require a higher degree of technical expertise. Some of the HiTET courses are also offered to state and local law enforcement personnel through the Law Enforcement Online (LEO) secure information sharing portal.

SANS Institute

FBI officials told us that the FBI had changed its training curriculum in response to recommendations in the OIG's 2011 report. Our report identified issues related to the format of the FBI's cyber development plan that could impede an agent's ability to acquire the training needed to investigate national security intrusion incidents effectively. One FBI official told us in the course of this review that the FBI is now focused on identifying the core skills cyber agents need and ensuring they receive proper training. As part of this effort, the FBI entered into a contract with the SANS Institute (SANS), a private company that specializes in information security and cyber security training.

FBI headquarters personnel cited several benefits of the SANS training. SANS frequently revises its courses and course offerings to provide professionals with the tools necessary to stay current in the ever changing cyber environment. SANS also offers regional training courses and in-house training for FBI personnel. The FBI eventually would like to expand the SANS training to state and local law enforcement agencies. One official told us that the new training model makes it easier to stay current with the changes in the constantly evolving field of cyber intrusions. Throughout our fieldwork, FBI cyber personnel consistently identified SANS as offering the best, most up-to-date training available. In addition, in a 2013 FBI-wide training survey, 81 percent of respondents cited SANS courses as the most beneficial for cyber professionals.

Master's Degree Programs

The FBI offers opportunities for qualified FBI personnel to enter a 2-year program to earn a Master of Science degree in Information Technology (MSIT) from Carnegie Mellon University. Currently there are 8 FBI personnel enrolled in the MSIT program and the FBI plans to expand the offer to accommodate up to 15 people in 2015. As part of the program, personnel must agree to a 3-year service commitment to the FBI to investigate cyber intrusion threats following graduation from the program. As referenced above, the FBI also is in the process of initiating a similar program at the New York University Polytechnic School of Engineering, in which up to six qualified FBI personnel may enroll. As of January 2015, no FBI

personnel had been selected to enroll in the program. While the numbers in these programs are small, we believe they may provide an attractive incentive and valuable training to help recruit, develop, and retain a core cadre of FBI cyber professionals.

Cyber Training Survey

In anticipation of the 2013 federal budget sequestration, which was expected to severely limit training resources, the FBI increased use of online training courses in its cyber curriculum. In August 2013, to gain a better understanding of the training needs of the cyber workforce, the FBI surveyed approximately 1,400 personnel with cyber responsibilities and received 1,154 responses (a response rate of approximately 82 percent). The results were compiled and documented in a November 2013 internal Cyber Division report.[11] We reviewed the report and found that the majority of respondents investigating cyber matters were relatively new to their position (reporting less than 5 years of experience in their current FBI position). The report noted that more than 80 percent of respondents preferred classroom courses. In addition, all of those respondents who reported they were working on cyber matters expressed a strong interest in advanced cyber training. The most requested training courses offered by SANS were: *Cutting-Edge Hacking Techniques*; *Network Penetration Testing*; and *Hacker Techniques, Exploits and Incident Handling*.

We were told by the FBI that based on responses to the survey, the cyber curriculum was revised and approved in November 2014. According to the FBI, the new cyber curriculum is based on several findings from the training survey, including: (1) designing the curriculum so that individuals from different academic and technical backgrounds can be trained to be cyber investigators; (2) balancing the technical courses offered by SANS and other investigative training courses; and (3) an overwhelming preference for classroom-based training, especially higher-level technical courses.

Computer Scientists

To strengthen its abilities to address the growing cyber threat and evolving technology, the FBI developed the Computer Scientists Field Operations Program to try to ensure adequate resources are available to enhance investigative and intelligence operations related to cyber intrusion threats. To address this requirement, during the fourth quarter of FY 2012 as part of the Next Gen Cyber Initiative, the FBI realigned its internal funded staffing levels (FSL) to include at least one computer scientist in each field office.

Due to a FY 2014 enhancement, the Cyber Division was authorized to hire 134 Computer Scientists to address the need for advanced cyber skills within the FBI. The FBI is currently hiring and training computer scientists. The goal is to

[11] Federal Bureau of Investigation Cyber Division Cyber Training and Logistics Unit, *Cyber Training Survey Data*, November 8, 2013.

assign at least 1 computer scientist to Cyber Task Forces in each of the 56 field offices. As of January 2015, however, 52 of the 134 Computer Scientist positions remained vacant and 5 of 56 field offices did not have at least 1 computer scientist, as planned.

All newly hired computer scientists are required to attend a 7-week training program at the FBI Academy in Quantico, Virginia. The objective is to teach computer scientist personnel how to apply their technical expertise in support of FBI investigations and operations. Since the implementation of the Next Gen Cyber Initiative, there have been four training cycles of the Computer Scientists Field Operations Program.

We were told by the FBI that because of the FY 2013 federal budget sequestration and government-wide hiring freeze, it has taken more time than originally anticipated to meet the intended computer scientist hiring goal. The FBI is also trying to hire more computer scientists from within the FBI and has listed vacancy announcements soliciting current FBI personnel to fill computer scientist positions.

The Assistant Director of the Cyber Division acknowledged that computer scientist position pay scales cannot compete with private sector pay scales. Therefore, in FY 2015 the Cyber Division requested and provided justification to hire four senior level positions under the Senior Level and Scientific Position (SL/ST) pay system to attract high-level, technically trained subject matter experts that are extremely difficult to recruit under the standard general pay scale.[12] Currently, the FBI employs contractors and cyber professionals to fulfill these highly technical positions. We were told by the FBI that the Senior Level and Scientific positions would provide it with a better opportunity to retain these highly skilled FBI cyber professionals, as well as provide a financial savings by potentially converting FBI contractor employees to government positions.

In addition to identifying alternate higher pay scales, the FBI is currently reviewing programs used by other agencies to attract qualified computer scientists, including programs that the NSA and CIA use to develop and attract high school students.

[12] Senior Level (SL) positions require individuals whose duties are broad and complex enough to be classified above the GS-15. Scientific or Professional (ST) positions require individuals with high-level research and development experience in physical, biological, medical, or engineering sciences, or a closely related field.

Expansion of Cyber Task Forces

Cyber Task Forces play an important role in the FBI's efforts to investigate and respond to significant cyber incidents. Although Cyber Task Forces have been established under the Next Gen Cyber Initiative in each of the 56 field offices, the FBI faces significant challenges in recruiting external partners to join the Cyber Task Forces. According to the FBI, few state and local agencies are predisposed to join a task force focused on cyber intrusions because they may not fully understand the cyber threat, they may believe that cyber intrusions are inherently a federal matter, or they may not have resources or personnel to detail an officer to the local Cyber Task Force. However, cyber intrusions affect businesses and individuals throughout the United States. The FBI's ability to coordinate domestic cyber threat information in local communities and respond to cyber incidents may be hindered by its inability to successfully recruit state and local partners on a consistent basis.

Cyber Task Forces

Prior to October 2012, Cyber Crime Task Forces were established in 45 of the 56 FBI field offices as part of the FBI's Cyber Crime Program. These task forces were responsible for investigating computer related crimes, including child pornography, theft of intellectual property, internet money laundering, gambling, and extortion. One of the objectives of the Next Gen Cyber Initiative was to redirect existing cyber squad resources to focus on cyber intrusion threats and incidents and establish a Cyber Task Force to do this work in each of the 56 field offices. After the Next Gen Cyber Initiative launched in October 2012, the FBI's Cyber Crime Program transitioned to the Criminal Investigative Division and the Cyber Division was restructured to focus solely on cyber intrusions.

Consequently, Cyber Task Forces were established in all of the 56 FBI field offices and focused exclusively on cyber intrusions. Also, FBI cyber intrusion program management was centralized within the FBI Cyber Division. According to an FBI official, the Cyber Task Force is the unifying structure at the field office level that aggregates all personnel working computer intrusion threats. Cyber Task Forces, led by a Cyber Squad Supervisor, work on computer intrusion threats and incidents and are comprised of FBI personnel and personnel detailed from other agencies.[13] One FBI official described each Cyber Task Force as a multi-disciplinary, cross-program, and multi-agency team that synchronizes the efforts of those with a role in cyber investigations. According to the Assistant Director of the Cyber Division, the case load for Cyber Task Forces is about 54 percent criminal-related matters and 46 percent national security-related matters.

[13] The personnel assigned to a Cyber Task Force may include Special Agents, Intelligence Analysts, Computer Scientists, and other professional staff from the FBI; and Task Force Officers, Task Force Members, and Task Force Participants detailed from other agencies.

According to FBI officials, the cyber intrusion threat has become increasingly relevant to state and local law enforcement agencies since entities targeted for cybercrime are located within state and local law enforcement agencies' areas of responsibilities. For example, in June 2014, the GameOver Zeus botnet targeted businesses and consumers throughout the United States, which resulted in complaints to state and local law enforcement agencies. The FBI's Cyber Task Forces are designed to lead interagency efforts to combat criminal and national security related cyber intrusion threats. As a result, the FBI seeks national, state, and local agency-level participation. Participants do not have to be sworn law enforcement officers. Civilian employees such as computer scientists and analysts working in the private sector, academic institutions, or other government agencies, such as the NSA, may be detailed to the Cyber Task Forces.

However, we found that the FBI has encountered challenges in attracting external participants to its Cyber Task Forces. According to the FBI, few state and local law enforcement agencies are motivated to join a task force focused on cyber intrusion threats because they may not fully understand the cyber threat, they may believe that cyber intrusion investigations are inherently a federal matter, or they may not have the resources or personnel to detail an officer to the local Cyber Task Force.

One FBI official stated that although state and local law enforcement agencies may not see cyber intrusion threats as an important concern, it will become more of an issue for them in the near future as cyber intrusions increase and the effects of those intrusions are felt at the state and local level. We were told by the FBI that the lack of external participation on Cyber Task Forces in each of the FBI's field offices may limit the sharing of critical information and hinder the FBI's ability to adequately investigate and address future cyber intrusion threats. As a result, the FBI told us that it is continuing its outreach efforts to educate state and local law enforcement agencies about the importance of this work by sharing information through cyber security briefings and offering cyber security training opportunities. We reviewed outreach materials and found that the materials address the domestic threat landscape and the tools used to identify the threats.

According to information reported by the field offices to the FBI Cyber Division, as of January 2015, the FBI had 1 Cyber Task Force in each of its 56 field offices. The Cyber Task Forces include over 1,000 members nationwide, representing over 80 state and local agencies, over 30 private sector entities, 6 academic institutions, and over 40 federal agencies, including the U.S. Secret Service, the NSA, and the CIA. In comparison, as of January 2015, the FBI had 71 Joint Terrorism Task Forces (JTTF) focused on investigating terrorism located in 104 cities nationwide, with at least 1 in each of the FBI's 56 field offices. According to the FBI's website, the JTTFs include approximately 4,000 members nationwide from over 500 state and local agencies and 55 federal agencies, including the Department of Homeland Security, the United States military, Immigration and Customs Enforcement, and the Transportation Security Administration.

In addition to the challenges mentioned above, FBI Cyber Division headquarters communications with the FBI field offices may have lacked sufficient

detail about the resources available to facilitate such participation. As result, field offices may have failed to consistently interpret the resources available for recruiting TFOs. For example, at two of the field offices we visited, FBI officials told us that one of the challenges in recruiting state and local participation is that they are unable to offer incentives to TFOs. However, at another field office, a TFO told us that the FBI provided use of computers, a government vehicle, and cyber training as incentives to attract TFOs to the Cyber Task Force. Additionally, the same TFO stated that the FBI field office provided additional resources, such as access for his local agency to the field office Computer Analysis Response Team (CART) lab examiners who process evidence.[14] We believe that the Cyber Division should ensure that all field offices are fully informed of the resources available to facilitate such participation.

While we are concerned about the lack of non-FBI representation on a number of Cyber Task Forces, there are signs that the FBI's efforts to bring in personnel from other agencies are yielding some results. In addition to the recruitment efforts for personnel from state and local agencies, in June 2014, the Assistant Director of the FBI Cyber Division told us that the NSA is in the process of selecting a total of six analysts to assign to Cyber Task Forces based in the San Antonio, Chicago, Atlanta, Detroit, San Francisco, and Pittsburgh field offices. One field office we visited had a Special Agent from the Department of Defense Office of the Inspector General assigned to its Cyber Task Force. Another field office had two part-time analysts from the United States Cyber Command. While these are positive developments, we believe the FBI needs to continue its efforts to educate and make it possible for other important partners, particularly including state and local law enforcement partners, to participate on the Cyber Task Forces and ensure all relevant Cyber Task Force information, including resources

[14] FBI's CART examiners provide digital forensic services to FBI investigators and, in certain instances, federal, state, and local partners. CART examiners analyze digital media including desktop and laptop computers, CDs/DVDs, and other forms of digital evidence.

available to attract external TFO participation, is consistently communicated by all field offices to facilitate that effort.[15]

Cyber Division Headquarters Reorganization

According to the FBI Cyber Division's Assistant Director, the FBI Cyber Division headquarters needs to do a better job of disseminating information to the field offices. At the start of our audit, Cyber Task Force personnel told us that the roles and responsibilities of officials at the FBI Cyber Division headquarters were not clearly communicated to the field. We believe one factor that may be exacerbating the communication issues is the repeated reorganization of the FBI Cyber Division. During the 15 months of our audit work, the FBI Cyber Division reorganized three times. Although we were repeatedly told that the Next Gen Cyber Initiative is constantly evolving, FBI personnel in the field divisions expressed frustration with the repeated changes to the management and organizational structure. While we believe that remaining agile is important in the rapidly evolving cyber domain, we also believe that such repeated reorganization can be confusing and disruptive to the field office personnel, especially if the reasons for the reorganizations and the new roles of various parts of Division headquarters are not communicated effectively. Understanding that the Next Gen Cyber Initiative is a proactive effort to address cyber threats, we believe that the FBI should ensure that any changes within the Cyber Division organizational structure, including roles and responsibilities, are clearly communicated to the field divisions.

[15] On September 8, 2014, the OIG briefed the FBI on the audit findings. At that time, the FBI did not provide any information related to Cyber Task Forces. At the exit conference conducted in May 2015, the FBI provided the OIG with documentation outlining steps that it has taken to fully inform each field office of resources available to facilitate and enhance task force participation. Specifically, the FBI told us in May 2015 that, in September 2014, it had launched an enhanced webpage as an information resource that included the Cyber Task Force Policy and Guidance Manual, Cyber Task Force Funding, Cyber Task Force FAQs, a Cyber Task Force Fact Sheet, and procedures for new Cyber Task Force Officers.

Private Sector Outreach and Coordination

The FBI has undertaken efforts to enhance its private sector outreach and coordination. However, interviews with representatives from major private sector firms revealed that the FBI continues to face challenges in sharing information and in developing mutually beneficial private sector partnerships. These private sector firms reported that information sharing seems to flow in one direction – from the private sector to the FBI. These private sector firms also reported that the information that is provided by the FBI to the private sector is information they already have access to or is not useful because it lacks context or is outdated. We found that contributing to the challenges with sharing information are private sector partners concerns about how any shared information will be used by the United States government. In particular, FBI officials and private sector representatives both acknowledged information sharing challenges related to balancing national security and individual privacy. The private sector reluctance to share information has been further affected by the distrust of government following the Edward Snowden leaks.[16]

Information Sharing and Collaboration

As part of the Next Gen Cyber Initiative, the FBI identified the need to enhance its efforts to develop private sector partnerships through outreach and collaboration. In public remarks at a February 2014 conference, FBI Director James B. Comey, Jr. acknowledged the need to combine the strengths of the private sectors' technical expertise, infrastructure, and innovation with the FBI's intelligence and law enforcement capabilities in order to combat the cyber threat.[17]

Several units within the FBI Cyber Division's Operations and Outreach Section are involved in the FBI's efforts to enhance private sector outreach and collaboration, including: (1) the National Industry Partnership Unit (NIPU); (2) the Guardian Victim Analysis Unit (GVAU); and (3) the Key Partnership Engagement Unit (KPEU).

[16] Edward Snowden is an American computer professional who worked at the NSA as a contractor and revealed classified information, including details of global surveillance programs. Snowden has been charged by the Department of Justice with violating the Espionage Act and theft of government property. United States v. Edward J. Snowden, 1:13 CR 265 (CMH).

[17] James B. Comey, Jr., Director, Federal Bureau of Investigation, Prepared Remarks (presented at the RSA Conference, San Francisco, California, February 26, 2014).

Cyber Division Outreach

We interviewed officials from the FBI Cyber Division NIPU, GVAU, and KPEU. The NIPU is responsible for facilitating information between the public and private sectors by disseminating information using the InfraGard Network.[18] The GVAU is responsible for the administration of Guardian, which is a centralized cyber intrusion tracking system.[19] Guardian allows the FBI to centralize, de-conflict, and locate all domestic cyber victim information and to coordinate notification to the field divisions by using the system to maintain a repository for cyber victims. The KPEU develops targeted partnerships with key private sector companies. Both Unit Chiefs of the NIPU and the KPEU told us that they frequently interact with NCIJTF and, when key private sector partners are identified, both units work with the NCIJTF to schedule briefings to educate and to further engage in future coordination.[20]

Although we found that the above mentioned FBI Cyber Division units work with private sector companies, private sector specific associations, and national level Information Sharing Analysis Centers to gain a strategic look at their respective sectors and to work to address cyber events and to provide industry information regarding cyber intrusions, we were told by FBI officials that it is the outreach that occurs at the field division level that yields the most effective results. One private sector official told us that his company's successful relationship with the FBI is in large part due to the outreach of the FBI special agent in the local field office.

National Cyber-Forensics and Training Alliance

The National Cyber-Forensics and Training Alliance (NCFTA), a Section 501(c)3 nonprofit organization, was established in 1997 to address the issue of cybercrime and functions as a conduit between the private sector and law enforcement to identify, mitigate, and neutralize cybercrime. The FBI Cyber Division's Cyber Initiative and Resource Fusion Unit (CIRFU) are co-located at the NCFTA in Pittsburgh, Pennsylvania.[21] The CIRFU is intended to combine the resources of federal law enforcement and private sector partners to identify and

[18] The InfraGard network is a longstanding partnership between the FBI and the private sector. It is a network of individuals dedicated to sharing information and intelligence to prevent hostile acts against the United States.

[19] Guardian is an FBI-wide incident and victim tracking system.

[20] According to information provided to the OIG after the exit conference in May 2015, from September 2013 through May 2015 the FBI provided a total of 111 classified briefings to 570 private sector entities and 145 unclassified briefings to 346 companies. Additionally, at the exit conference, the FBI told us it is codifying its processes for outreach to the private sector through an enterprise-wide initiative. The Cyber Division is collaborating with the Office of Private Sector Engagement on this initiative, and its methodology to identify and prioritize outreach is being adopted by the Office of Private Sector Engagement.

[21] In June 2014, the CIRFU was moved from the Cyber Division's Cyber Outreach Section to the Cyber Operation Section.

combat significant actors involved in both criminal and national security threats. NCFTA members develop strategies to mitigate the cyber threat and the CIRFU uses that information to open or further existing FBI investigations, often together with law enforcement partners around the world.

The NCFTA Chief Executive Officer (CEO) told us that the NCFTA has been successful breaking down information sharing barriers between the private sector and government. The CEO indicated that in the past, private sector representatives felt that there was no mutual sharing of information. For example, the private sector would provide unclassified information to the FBI, which would subsequently mark it as classified and then not share the information with others in the private sector. The information shared and maintained at the NCFTA is considered unclassified and open source, which allows for greater collaboration between NCFTA members and the FBI. One private sector representative told us that the NCFTA is the gold standard for sharing information. According to the NCFTA CEO, there are about 15 private sector companies with representatives currently located at the NCFTA and it is in the process of recruiting an additional 19 new private sector companies.

We found that NCFTA participants rely heavily on the informal relationships that have resulted from members working in the same location. One NCFTA participant told us that discussions among NCFTA members often occur informally about threats without giving away sensitive or proprietary information. However, the same NCFTA participant told us that one of the challenges with information it receives from the FBI is that it is stale by the time it is formally distributed through one of FBIs intelligence reports to industry. Several NCFTA members said that a lot of the FBI information that should be available for sharing is over-classified, and that this prevents the timely sharing of information.

Challenges in Sharing Information

The FBI faces several challenges in sharing information with the private sector, including: (1) a perception by the private sector that information flows in one direction – to the FBI; (2) information, when provided by the FBI, is often not useful because it lacks context or is outdated; and (3) private sector concerns regarding how the FBI will use the information that is shared.

One-Way Communication of Information

At the February 2014 conference mentioned previously, Director Comey also acknowledged that it often seems to private industry that information flows one way – to the government.[22] We interviewed representatives from more than 12 private sector entities and were consistently told that information seems to only flow in one direction, which is from the private sector to the FBI. Several private sector representatives told us that providing information to the FBI is akin to sending it into a black hole – the information goes in and the entities never hear

[22] Comey, RSA Conference.

any more about it. The FBI has acknowledged these private sector concerns, but has also stated that a lot of information cannot readily be shared because it is part of an ongoing investigation. In response to this challenge, the FBI has developed reports that it can share with the private sector. According to the FBI, FBI Liaison Alert System Reports share anonymous and declassified technical indicators, gleaned from ongoing investigations, with the private sector to assist them with protecting their networks. From April 2013 through January 2015, 70 FBI Liaison Alert System Reports were disseminated. The FBI also disseminates Private Industry Notification Reports that provide contextual threat information regarding nefarious activity by cyber criminals. From May 2013 to January 2015, the FBI disseminated 42 Private Industry Notification Reports.

While this explanation may have some validity in certain cases, we believe that when the FBI fails to exchange information on an ongoing basis with the private sector, the private sector's ability to address and mitigate threats in a timely manner may be hindered. In addition, this lack of mutual exchange of timely information creates an environment in which private sector entities may be less willing to share important information in the future.

Outdated FBI Information

According to private sector representatives, another issue is the timeliness of information received from the FBI. Several private sector representatives stated that they believe that the FBI over-classifies its information and by the time the information is "scrubbed" and released, the information is often stale and no longer useful. They also told us that the information received from the FBI is often information that the private sector partners already have.

Another private sector representative told us that cybersecurity information has to move fast and that the FBI should determine a method for not over-classifying its information to facilitate this. Additionally, the same private sector representative told us that if the FBI does not have a metric in place to measure how quickly information is being disseminated from the FBI to the private sector, it should. We confirmed with the FBI that no such metrics exist but that the FBI was in the process of working to develop metrics to measure the efficiency with which information is shared. We believe that the FBI cannot measure its own effectiveness if it is not measuring the time from when it receives to when it disseminates actionable information to the private sector.

Director Comey stated that the FBI needs to have a means to share information in real time.[23] We found that the FBI is currently working on machine-to-machine capabilities that would facilitate sharing of cyber threat information in a more timely fashion with the private sector.[24] At the time of our fieldwork, the

[23] Comey, RSA Conference.

[24] Machine-to-machine communication is a broad label that describes the technology used to exchange information without the assistance of human intervention.

FBI's machine-to-machine capabilities were still in the planning stages. One private sector representative told us that many private sector entities are already using machine-to-machine platforms and the FBI should consider doing so to provide more timely information to the private sector. The representative added that in the cyber arena, that velocity of information is critical. Given the growing nature of the cyber threat, we recommend that the FBI move as quickly as possible to develop strategies, including machine-to-machine capabilities to ensure the timely dissemination of actionable information to the private sector.

Challenges to Outreach and Collaboration

In planning the Next Gen Cyber Initiative, the FBI anticipated that private sector partners would be reluctant to provide the FBI with access to data that may contain personally identifiable information (PII).[25] During our interviews with private sector individuals, we found that private sector entities are reluctant to share information, such as PII or sensitive or proprietary information, with the government because of concerns about how that information could be used or the possibility that it could be publicly released under the Freedom of Information Act (FOIA).[26] One private sector professional told us that he had declined to be interviewed by the OIG due to FOIA concerns.

In addition, several private sector individuals discussed with us the challenges in collaborating with the FBI in a "post-Snowden" era. One private sector individual emphasized that Snowden has redefined how the private sector shares information with the United States government. We were told by private industry representatives and the FBI that, following the Snowden disclosures, private sector entities have become more reluctant to share information with the United States government because they are uncertain as to how the information they provide will be used and are concerned about balancing national security and individual privacy interests.

The FBI Director has acknowledged private sector concerns related to proprietary information and the need to guard customer data and stated the FBI will do what it can to protect private sector privacy.[27] More generally, efforts to detect, prevent, and mitigate threats are hampered because neither the public nor private sector can see the whole picture. The FBI Director further explained the

[25] According to the National Institute of Standards and Technology, PII is personal information about an individual consisting of (1) information that can be used to distinguish or trace an individual's identify, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

[26] The Freedom of Information (FOIA) Act, 5 U.S.C. § 552, is a law that allows for the full or partial disclosure of previously unreleased information and documents controlled by the United States government. FOIA explicitly applies only to executive branch government agencies. FOIA defines agency records subject to disclosure and grants nine exemptions which address issues of sensitivity and personal rights.

[27] Comey, RSA Conference.

government lacks visibility into the many private networks maintained by companies in the United States, and the FBI "has information it cannot always share [with the private sector]." Consequently, each can see distinct types of cyber threats, but the information is not always visible to the other. We believe that the FBI should strengthen its outreach efforts to provide appropriate assurances regarding its handling of PII and proprietary information received from the private sector and work to reduce classification, where appropriate, of information in its possession in order to improve sharing and collaboration in both directions consistent with appropriate privacy and other limitations.

Conclusion

Overall, we determined that the FBI has made considerable progress towards achieving the goals it established for the Next Gen Cyber Initiative. We found that the FBI appears to have strengthened the NCIJTF by adding international participation, reorganizing to eliminate the perception that the NCIJTF is an extension of the Cyber Division, and improving information sharing. However, we believe the FBI should develop a process to track and measure the timeliness of information sharing.

We found that, as part of the Next Gen Cyber Initiative, the FBI has implemented a new training strategy to improve the awareness of all FBI employees, as well as the technical capabilities of those investigating cyber intrusion threats and incidents. We also found that the FBI continues to make efforts to recruit, develop, and retain its cyber workforce. While we found that the FBI is participating in various recruitment events, recruitment of qualified candidates remains a challenge for the FBI. In addition, we found that retaining highly qualified personnel can be a challenge when private sector entities can pay higher salaries and applicants do not have to undergo the same background investigation process as with the FBI. We believe that the FBI should continue its creative recruitment and retention efforts, including targeted use of the SLRP and increase the mobility of former employees with critical skills, to attract and retain highly skilled cyber professionals. Further, we believe that the FBI needs to continue to identify and recruit professionals who are motivated by the FBI's mission as opposed to higher salaries. We also found that the FBI has not hired the full complement of computer scientists for which it was authorized, and that it should increase its efforts to address this.

Similarly, while we found that the FBI's Next Gen Cyber Initiative has met its objective to establish Cyber Task Forces in all 56 field offices, challenges remain. Specifically, we found that recruitment of external participants, particularly from state and local law enforcement remains a challenge for the FBI. We believe that the FBI should continue its outreach efforts to attract these external participants to its Cyber Task Forces in order to foster information sharing and further the Cyber Task Force's ability to fully investigation and address future cyber intrusion threats. In addition, we believe that the Cyber Division should ensure that all field offices are fully informed of the resources available to facilitate such participation. The FBI also should ensure that the Cyber Division organization and lines of authority, and any changes in same, are clearly communicated to all field offices.

Lastly, we found that the FBI has made efforts to establish some informal relationships for sharing information with private sector partners; however, we believe that the FBI should continue to strengthen its efforts to share and collaborate with the private sector. In addition, we believe that the FBI should continue its efforts to develop strategies, including machine-to-machine capabilities to enable the more timely dissemination of information to the private sector. We also believe the FBI should develop a metric to measure the time it receives information to the time it makes the information actionable.

Recommendations

We recommend that the FBI:

1. Develop a process to track and measure the timeliness of information sharing at the NCIJTF.

2. Increase its efforts to hire computer scientists for authorized positions.

3. Continue to develop creative strategies for recruiting, hiring, and retaining highly skilled cyber professionals, including cyber agent targeted recruitment efforts, new computer scientist job series, and using external partners to identify highly qualified candidates motivated by a career in the FBI.

4. Continue its outreach efforts to recruit detailees to its Cyber Task Forces, including ensuring that information about resources available to facilitate partner agency participation is effectively communicated.

5. Ensure that changes within the Cyber Division organizational structure, including roles and responsibilities, are clearly communicated to the field divisions.

6. Continue to strengthen its outreach efforts to improve sharing and collaboration with private sector entities.

7. Develop metrics to measure the timeliness with which it provides actionable information to the private sector.

8. Move promptly to develop strategies, including machine-to-machine capabilities, to ensure the timely dissemination of actionable information to the private sector.

STATEMENT ON INTERNAL CONTROLS

As required by the *Government Auditing Standards*, we tested, as appropriate, internal controls significant within the context of our audit objective. A deficiency in an internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to timely prevent or detect: (1) impairments to the effectiveness and efficiency of operations, (2) misstatements in financial or performance information, or (3) violations of laws and regulations. Our evaluation of the Federal Bureau of Investigation's (FBI) internal controls was *not* made for the purpose of providing assurance on its internal control structure as a whole. FBI management is responsible for the establishment and maintenance of internal controls.

Through our audit testing, we did not identify any deficiencies in the FBI's internal controls that are significant within the context of the audit objective and based upon the audit work performed that we believe would affect the FBI's ability to effectively and efficiently operation, to correctly state financial and performance information, and to ensure compliance with laws and regulations.

Because we are not expressing an opinion on the FBI's internal control structure as a whole, this statement is intended solely for the information and use of the FBI. This restriction is not intended to limit the distribution of this report, which is a matter of public record.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

As required by the *Government Auditing Standards* we tested, as appropriate given our audit scope and objective, selected transactions, records, procedures, and practices to obtain reasonable assurance that the Federal Bureau of Investigation's (FBI) management complied with federal laws and regulations, for which noncompliance, in our judgment, could have a material effect on the results of our audit. FBI's management is responsible for ensuring compliance with applicable federal laws and regulations. In planning our audit, we identified the following laws and regulations that concerned the operations of the auditee and that were significant within the context of the audit objective:

- Computer Fraud and Abuse Act of 1986;
- Executive Order 13636;
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23.

Our audit included examining, on a test basis, the FBI's compliance with the aforementioned laws and regulations that could have a material effect on the FBI's operations, through interviewing FBI personnel, analyzing data, examining procedural practices, and assessing internal control procedures. Nothing came to our attention that caused us to believe that the FBI was not in compliance with the aforementioned laws and regulations.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective of our audit was to evaluate the Federal Bureau of Investigation's (FBI) implementation of its Next Generation Cyber (Next Gen Cyber) Initiative.

Scope and Methodology

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our audit focused on the FBI's implementation goals for the Next Gen Cyber Initiative including: (1) strengthening the National Cyber Investigative Joint Task Force; (2) advancing the capability of the FBI cyber workforce and supporting enterprise infrastructure; (3) expanding the Cyber Task Forces focused on intrusions in each of the FBI's 56 field offices; and (4) enhancing information sharing and operational collaboration with the private sector. The scope of our review primarily encompasses May 2012 through January 2015.

To accomplish our audit objective, we interviewed responsible staff members in the FBI's Cyber Division, Counterintelligence Division, Directorate of Intelligence, Training Division, Operational and Technology Division, Finance Division, Resource Planning Office, and Inspection Division. We also interviewed officials from the U.S. Department of Justice National Security Division and National Cyber Investigative Joint Task Force members, including the U.S. Air Force Office of Special Investigations, Central Intelligence Agency, U.S. Cyber Command, U.S. Department of Homeland Security, National Security Agency, and Five Eyes representatives from Australia and the United Kingdom.

We reviewed Next Gen Cyber Initiative planning documentation, records, and reports. In addition, we conducted site visits and interviewed responsible officials, at FBI field offices in Newark, New Jersey; Philadelphia, Pennsylvania; Pittsburgh, Pennsylvania; San Francisco, California; and Seattle, Washington. To evaluate the FBI's efforts at expanding its Cyber Task Forces, we interviewed external FBI Cyber Task Force members.

We evaluated the FBI's efforts at outreach and collaboration with the private sector and interviewed responsible officials from more than 12 private sector entities, including the National Cyber-Forensics and Training Alliance and Carnegie Mellon University's Software Engineering Institute.

FEDERAL BUREAU OF INVESTIGATION'S RESPONSE TO THE DRAFT AUDIT REPORT

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

July 20, 2015

The Honorable Michael E. Horowitz
Inspector General
Office of the Inspector General
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530

Dear Mr. Horowitz:

The Federal Bureau of Investigation (FBI) appreciates the opportunity to review and respond to your office's report entitled, "*Audit of the Federal Bureau of Investigation's Implementation of Its Next Generation Cyber Initiative.*"

We are pleased you found the FBI's "Next Gen Cyber Initiative represents a fundamental shift in the FBI's approach to addressing the cyber threat, changing focus from reacting to cyber-attacks to predicting and preventing them." As you determined, "information sharing has improved" among the members of the National Cyber Investigative Joint Task Force (NCIJTF); "Cyber Task Forces" have been established at all 56 FBI Field Offices; a "cyber-specific training strategy" has been implemented to improve the technical skills of our entire workforce; and "creative recruitment and retention efforts" have been made to attract and retain highly skilled cyber professionals. These significant steps have helped the FBI get ahead of the many cyber intrusions challenges.

Our "lean forward" approach under the Initiative has also extended to the private sector. As noted, since September 2013, the FBI has provided 256 briefings to over 900 private sector companies to provide relevant, valuable, and timely information outside the FBI. To effectuate those briefings which were classified, the FBI also enabled temporary access to classified information to approximately 350 of these private sector partners. Additionally, through our FBI Liaison Alert System (FLASH) Reports, we have broadly shared 70 anonymous and declassified technical indicators for immediate action to protect critical networks. Over 40 Private Industry Notification (PIN) Reports have also been released to private sector components including contextual threat information regarding nefarious activity by cyber threat actors.

The FBI remains dedicated to applying the highest level of technical capability and investigative expertise toward combating cyber-based intrusions targeting the United States. Our Human Resources Division continues to develop aggressive and innovative recruitment and retention strategies in collaboration with our Intelligence Community partners, as the cyber workforce challenge runs throughout the federal government.

We appreciate the professionalism of your audit staff throughout the review and concur with each of the recommendations, many of which we have already taken actions to implement. Should you have any questions, please feel free to contact me.

Sincerely,

Joseph M. Demarest
Associate Executive Assistant Director
Criminal, Cyber, Response and
Services Branch

THE FEDERAL BUREAU OF INVESTIGATION'S IMPLEMENTATION OF ITS NEXT GENERATION CYBER INITIATIVE

Recommendation #1: Develop a process to track and measure the timeliness of information sharing at the NCIJTF.

FBI Response to Recommendation #1: Concur. The FBI will develop a process to track and measure the timeliness of information sharing at the NCIJTF.

Recommendation #2: Increase its efforts to hire computer scientists for authorized positions.

FBI Response to Recommendation #2: Concur. The Human Resources Division (HRD) will continue focusing on the aggressive hiring of Computer Scientists and other technical professionals to help Cyber Division best combat immediate and emerging threats. HRD is also integrating a tech-specific recruitment plan into the Bureau's larger, overarching recruitment plan, to include: targeted talent recruitment; developing partnerships with specific educational institutions, talent incubators and/or technical organizations that provide cyber training and credible [ethical] developmental opportunities, such as intrusion and defense competitions.

Recommendation #3: Continue to develop creative strategies for recruiting, hiring, and retaining highly skilled cyber professionals, including cyber agent targeted recruitment efforts, new computer scientist job series, and using external partners to identify highly qualified candidates motivated by a career in the FBI.

FBI Response to Recommendation #3: Concur. The FBI will continue to develop creative strategies for recruiting, hiring, and retaining highly skilled cyber professionals, including cyber agent targeted recruitment efforts, new computer scientist job series, and using external partners to identify highly qualified candidates motivated by a career in the FBI.

Recommendation #4: Continue its outreach efforts to recruit detailees to its Cyber Task Forces, including ensuring that information about resources available to facilitate partner agency participation is effectively communicated.

FBI Response to Recommendation #4: Concur. The FBI will continue its outreach efforts to recruit detailees to its Cyber Task Forces, including ensuring that information about resources available to facilitate partner agency participation is effectively communicated.

Recommendation #5: Ensure that changes within the Cyber Division organizational structure, including roles and responsibilities, are clearly communicated to the field divisions.

FBI Response to Recommendation #5: Concur. The FBI will ensure that changes within the Cyber Division organizational structure, including roles and responsibilities, are clearly communicated to the field divisions.

Recommendation #6: Continue to strengthen its outreach efforts to improve sharing and collaboration with private sector entities.

FBI Response to Recommendation #6: Concur. The FBI will continue to strengthen its outreach efforts to improve sharing and collaboration with private sector entities.

Recommendation #7: Develop metrics to measure the timeliness with which it provides actionable information to the private sector.

FBI Response to Recommendation #7: Concur. The FBI will develop metrics to measure the timeliness with which it provides actionable information to the private sector.

Recommendation #8: Move promptly to develop strategies, including machine-to-machine capabilities to ensure the timely dissemination of actionable information to the private sector.

FBI Response to Recommendation #8: Concur. The FBI will move promptly to develop strategies, including machine-to-machine capabilities to ensure the timely dissemination of actionable information to the private sector.

OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT

The Department of Justice, Office of the Inspector General (OIG) provided a draft of this audit report to the Federal Bureau of Investigation (FBI). The FBI's response is incorporated in Appendix 2 of this final report. The following provides the OIG analysis of the response and summary of actions necessary to close the report.

Recommendations:

1. **Develop a process to track and measure the timeliness of information sharing at the National Cyber Investigative Joint Task Force (NCIJTF).**

   Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that it will develop a process to track and measure the timeliness of information sharing at the NCIJTF.

   This recommendation can be closed when we receive evidence that the FBI has developed a process to track and measure the timeliness of information sharing at the NCIJTF.

2. **Increase its efforts to hire computer scientists for authorized positions.**

   Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that the FBI Human Resources Division (HRD) will continue to focus on hiring computer scientists and other technical professionals to help the Cyber Division combat immediate and emerging threats. According to the FBI's response, the HRD is also integrating a technology specific recruitment plan into the FBI's larger, overarching recruitment plan, to include: (1) targeted talent recruitment; and (2) developing partnerships with specific educational institutions, talent incubators, and/or technical organizations that provide cyber training and credible developmental opportunities, such as intrusion and defense competitions.

   This recommendation can be closed when we receive evidence that the FBI has increased its efforts to hire computer scientists for authorized positions and other technical professionals to help combat immediate and emerging cyber threats.

3. **Continue to develop creative strategies for recruiting, hiring, and retaining highly skilled cyber professionals, including cyber agent targeted recruitment efforts, new computer scientist job series, and using external partners to identify highly qualified candidates motivated by a career in the FBI.**

Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that it will continue to develop creative strategies for recruiting, hiring, and retaining highly skilled cyber professionals, including cyber agent targeted recruitment efforts, new computer scientist job series, and using external partners to identify highly qualified candidates motivated by a career at the FBI.

This recommendation can be closed when we receive evidence that the FBI has developed creative strategies for retaining highly skilled cyber professionals.

4. **Continue its outreach efforts to recruit detailees to its Cyber Task Forces, including ensuring that information about resources available to facilitate partner agency participation is effectively communicated.**

Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that it will continue its outreach efforts to recruit detailees to it Cyber Task Forces, including ensuring that information about resources available to facilitate partner agency participation is effectively communicated.

This recommendation can be closed when we receive evidence that the FBI has continued its Cyber Task Force recruitment efforts and ensures that information about resources available to facilitate partner agency participation is effectively communicated.

5. **Ensure that changes within the Cyber Division organizational structure, including roles and responsibilities, are clearly communicated to the field divisions.**

Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that it will ensure that changes within the FBI Cyber Division organizational structure, including roles and responsibilities, are clearly communicated to the field divisions.

This recommendation can be closed when the FBI provides evidence that it ensures Cyber Division organizational changes are clearly communicated to the field divisions.

6. **Continue to strengthen its outreach efforts to improve sharing and collaboration with private sector entities.**

Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that it will continue to strengthen its outreach efforts to improve sharing and collaboration with private sector entities.

This recommendation can be closed when we receive evidence that the FBI is continuing to strengthen its outreach efforts to improve sharing and collaboration with private sector entities.

7. **Develop metrics to measure the timeliness with which it provides actionable information to the private sector.**

   Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that it will develop metrics to measure the timeliness with which it provides actionable information to the private sector.

   This recommendation can be closed when we receive evidence that the FBI has developed metrics to measure the timeliness with which it provides actionable information to the private sector.

8. **Move promptly to develop strategies, including machine-to-machine capabilities, to ensure the timely dissemination of actionable information to the private sector.**

   Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that it will move promptly to develop strategies, including machine-to-machine capabilities, to ensure the timely dissemination of actionable information to the private sector.

   This recommendation can be closed when we receive evidence that the FBI has developed strategies to ensure the timely dissemination of actionable information to the private sector.

The Department of Justice Office of the Inspector General (DOJ OIG) is a statutorily created independent entity whose mission is to detect and deter waste, fraud, abuse, and misconduct in the Department of Justice, and to promote economy and efficiency in the Department's operations. Information may be reported to the DOJ OIG's hotline at www.justice.gov/oig/hotline or (800) 869-4499.

Office of the Inspector General
U.S. Department of Justice
www.justice.gov/oig